ID: 385422
Sample Name:
UOB_BANK_MT104_SCAN.exe
Cookbook: default.jbs
Time: 13:41:12
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

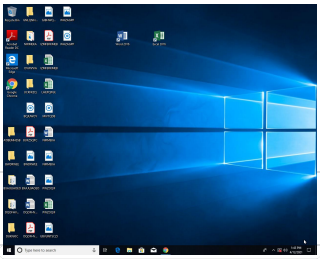
Analysis Report UOB_BANK_MT104_SCAN.exe

Overview

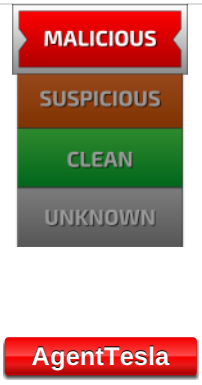
General Information

Sample Name:	UOB_BANK_MT104_SCAN.exe
Analysis ID:	385422
MD5:	62cffbe922a88eb..
SHA1:	56932184675967..
SHA256:	bcb425236d9708..
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

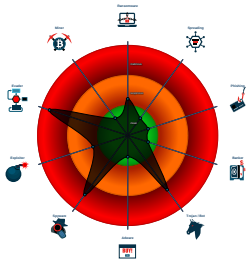


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- UOB_BANK_MT104_SCAN.exe (PID: 7164 cmdline: 'C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe' MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
  - UOB_BANK_MT104_SCAN.exe (PID: 976 cmdline: C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
  - UOB_BANK_MT104_SCAN.exe (PID: 6460 cmdline: C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
- outlook.exe (PID: 5832 cmdline: 'C:\Users\user\AppData\Roaming\outlook\outlook.exe' MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
  - outlook.exe (PID: 5948 cmdline: C:\Users\user\AppData\Roaming\outlook\outlook.exe MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
- outlook.exe (PID: 4684 cmdline: 'C:\Users\user\AppData\Roaming\outlook\outlook.exe' MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
  - outlook.exe (PID: 6832 cmdline: C:\Users\user\AppData\Roaming\outlook\outlook.exe MD5: 62CFFBE922A88EBAE13AB4AEBFD8ED2D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "datastore1840@yandex.comopjis0123smtp.yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.734707746.000000000290 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.653990292.0000000003E9 B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.897512069.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.901584866.00000000030E 2000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.900779830.0000000002DE1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 22 entries				

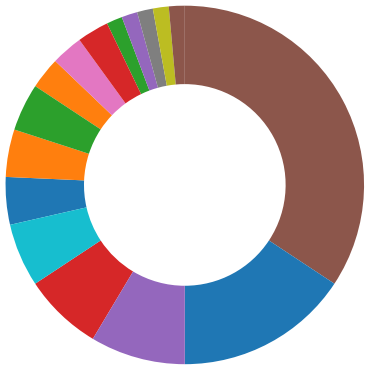
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.UOB_BANK_MT104_SCAN.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.outlook.exe.3b98490.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.outlook.exe.3b98490.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.outlook.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.outlook.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Moves itself to temp directory

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file access)

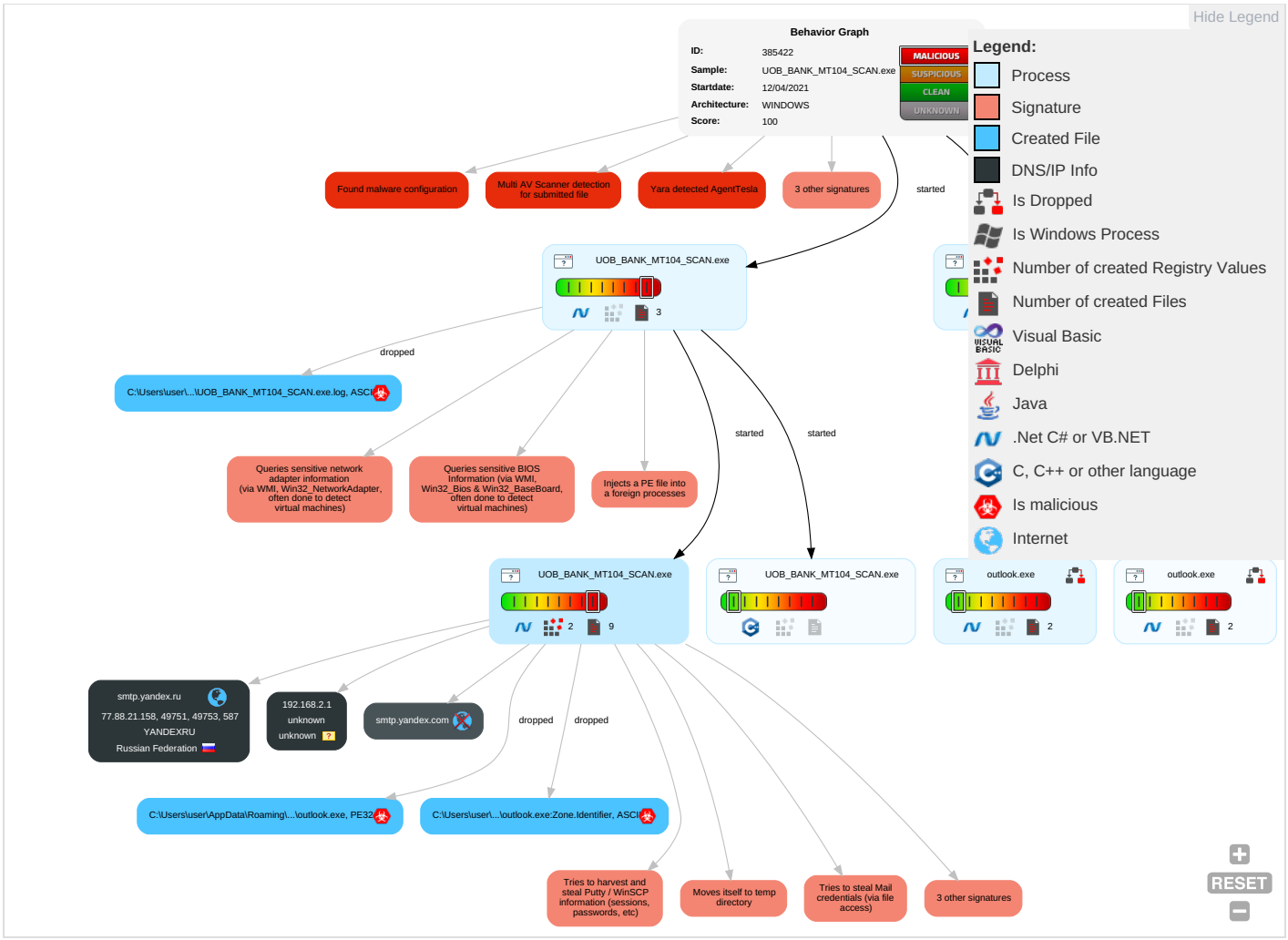
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

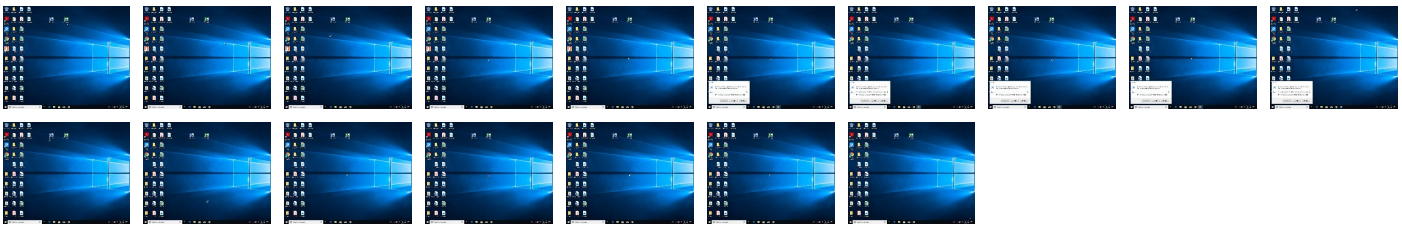
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
UOB_BANK_MT104_SCAN.exe	21%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.UOB_BANK_MT104_SCAN.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.outlook.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.2.outlook.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://eLwHQQ0svk5HHFd0MGv.net	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://crl.certum.	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.com%	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/fi-f	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://JaIZBT.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://yandex.crl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/o	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/A	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.900779830.0000000002DE1000.00000004.00000001.sdmp, outlook.exe, 0000000E.00000002.900334677.0000000002AE1000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.74236742 0.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.74236742 0.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.74236742 0.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://eLwHQQ0svk5HHFd0MGv.net	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.901584866.00000000030E2000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000005.00000002.902051622.000000000316A000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000005.00000003.856563037.00000000010C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.74236742 0.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://yandex.crl.certum.pl/ycasha2.crl0q	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.0000000000664A000.00000004.00000001.sdmp	false		high
http://subca.ocsp-certum	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.905675648.0000000006630000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://crl.certum.	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.905675648.0000000006630000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.74236742 0.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.653198971.0000000002D11000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.73470 7746.0000000002901000.00000004.00000001.sdmp, outlook.exe, 00000010.00000002.758186038.0000000002F01000.00000004.00000001.sdmp	false		high

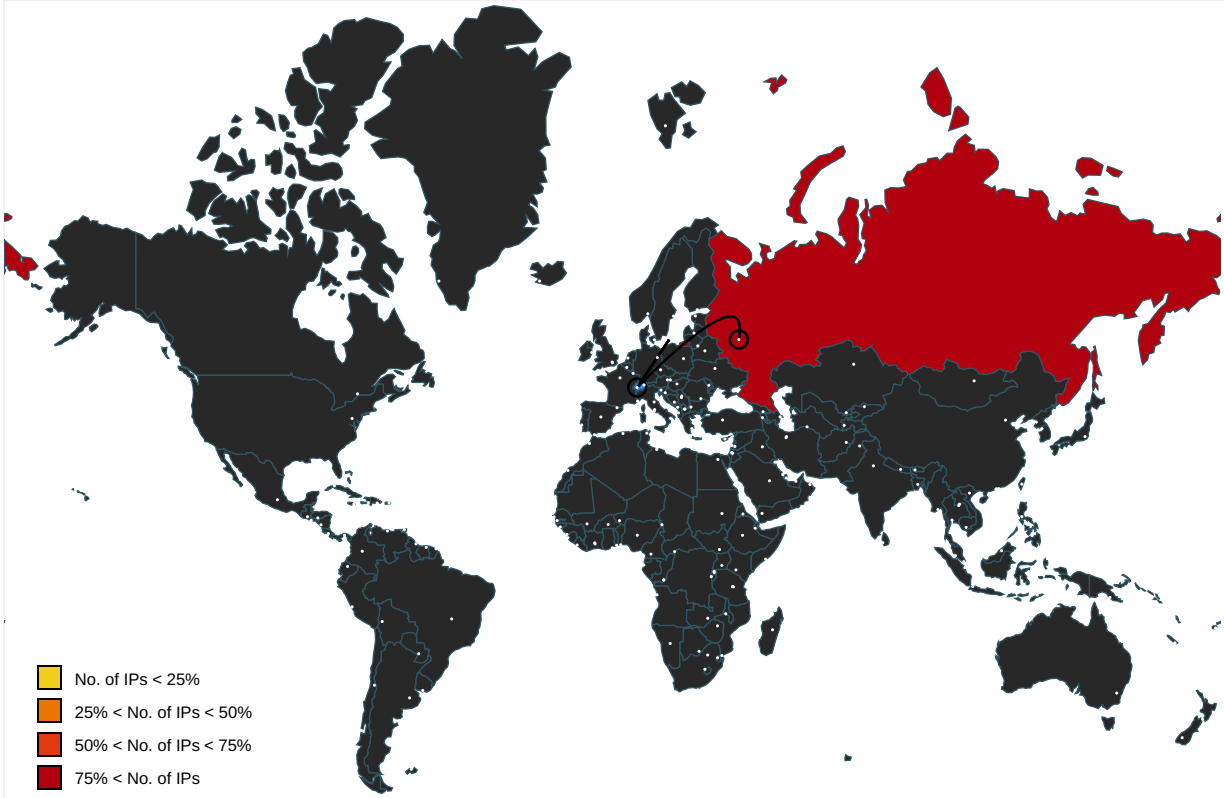
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://subca.ocsp-certum.com0.	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ca.cer09	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.640104709.0000000005BBA000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000000.00000003.635320982.0000000005BCB000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com%	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.655298585.0000000005BB7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://subca.ocsp-certum.com01	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comn	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.635092214.0000000005BCB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638623691.0000000005BB7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	outlook.exe, 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kr	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.653103625.000000002CC1000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.734583011.00000000028B1000.00000004.00000001.sdmp, outlook.exe, 00000010.00000002.757931967.0000000002EB1000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/fi-f	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.653990292.0000000003E9B000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000005.00000002.897472455.0000000000402000.00000040.00000001.sdmp, outlook.exe, 0000000B.00000002.736717665.0000000003A8B000.00000004.00000001.sdmp, outlook.exe, 0000000E.00000002.897512703.0000000000402000.00000040.00000001.sdmp, outlook.exe, 00000010.00000002.759764296.000000000408B000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.897512069.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certum.pl/CPS0	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.0000000000664A000.00000004.00000001.sdmp	false		high
http://repository.certum.pl/ycasha2.cer0	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.0000000000664A000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://JaIZBT.com	outlook.exe, 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.655298585.0000000005BB7000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	outlook.exe, 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnLog	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.636617989.0000000005BBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.900779830.0000000002DE1000.00000004.00000001.sdmp, outlook.exe, 0000000E.00000002.900334677.0000000002AE1000.00000004.00000001.sdmp, outlook.exe, 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false		high
http://yandex.crl	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/o	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/H	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.certum.pl/CPS0	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/A	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638623691.0000000005BB7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638438342.0000000005BB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.yandex.com	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.902115914.0000000003180000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%$	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.900779830.0000000002DE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://yandex.ocsp-responder.com03	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.000000000664A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/v	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638438342.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/%	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638438342.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://yandex.ocsp-rXj	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.905675648.0000000006630000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crls.yandex.net/certum/ycasha2.crl0-	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.0000000000664A000.00000004.00000001.sdmp	false		high
http://crls.yandex.net/certum/ycasha2.crl0LjZk)	UOB_BANK_MT104_SCAN.exe, 00000005.00000002.905675648.0000000006630000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638438342.0000000005BB4000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638623691.0000000005BB7000.00000004.00000001.sdmp, UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638410750.0000000005BBC000.00000004.00000001.sdmp, outlook.exe, 000000B.00000002.742367420.00000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	UOB_BANK_MT104_SCAN.exe, 00000000.00000002.656292638.0000000006DC2000.00000004.00000001.sdmp, outlook.exe, 0000000B.00000002.742367420.00000000059B0000.00000002.00000001.sdmp, outlook.exe, 00000010.00000002.763199162.0000000005ED0000.00000002.00000001.sdmp	false		high
http://crl.certum.pl/ca.crl0h	UOB_BANK_MT104_SCAN.exe, 00000005.00000003.873712639.0000000000664A000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/d	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.638292104.0000000005BBC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnrig	UOB_BANK_MT104_SCAN.exe, 00000000.00000003.636617989.0000000005BBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385422
Start date:	12.04.2021
Start time:	13:41:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UOB_BANK_MT104_SCAN.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/5@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 19.1% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 92.122.145.220, 104.43.193.48, 52.147.198.201, 13.64.90.137, 52.255.188.83, 20.82.209.183, 168.61.161.212, 92.122.213.194, 92.122.213.247, 205.185.216.42, 205.185.216.10, 104.42.151.234, 20.82.210.154, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:41:58	API Interceptor	719x Sleep call for process: UOB_BANK_MT104_SCAN.exe modified
13:42:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run outlook C:\Users\user\AppData\Roaming\outlook\outlook.exe
13:42:33	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run outlook C:\Users\user\AppData\Roaming\outlook\outlook.exe
13:42:38	API Interceptor	838x Sleep call for process: outlook.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	zq17jG57TX.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36663460.22787.exe	Get hash	malicious	Browse	
	Payment_Advice.exe	Get hash	malicious	Browse	
	Swift_Copy.exe	Get hash	malicious	Browse	
	C6RET8T1Wi.exe	Get hash	malicious	Browse	
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	Payment _Advice (2).exe	Get hash	malicious	Browse	
	cricket.exe	Get hash	malicious	Browse	
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	
	Shandong CIRS Form.exe	Get hash	malicious	Browse	
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	
	Q99Eljz7IT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	zq17jG57TX.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKD.36663460.22787.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment_Advice.exe	Get hash	malicious	Browse	• 77.88.21.158
	qINcOlwRud.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift_Copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	C6RET8T1Wi.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	zq17jG57TX.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKD.36663460.22787.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment_Advice.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift_Copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	C6RET8T1Wi.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 77.88.21.179
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UOB_BANK_MT104_SCAN.exe.log	
Process:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	
Process:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\outlook\outlook.exe	
Process:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	818176
Entropy (8bit):	7.692203118539672
Encrypted:	false
SSDEEP:	12288:SopTcgSA5FMxYj3yATy1nWPGNUsSvjHAE0diJHXbms5PulZWYNh3Cq4HrRDi4DHL:PTNHgYjiA21WL7PNas5PuyY/d4HNhmq
MD5:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
SHA1:	569321846759678308CB52D01537AEFC2D9D8389
SHA-256:	BCB425236D9708ACD844D3ABF15E14A33F029EE760D1DACF9C590A70C2283E75
SHA-512:	C383B9420D22FD87AAEDD9F5A157F8757ABF53EFB9D6CE724416AC26A4CBB21C59B7DA7DB2830B8F9F3B234B161DC026D25E55DC9F7D3D67DF45C8FC7256FC4
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...E.t`.....P..\.....>z... .....@.. ..... ..@.....y..O.....T..... ..... ..H.....text...\Z... ...\..... ..`.rsrc...T.....^.....@..@.rel oc.....z.....@..B..... z.....H.....d.....0.....($...(%.....(....o&....*.....('.....((.....()....(*.....(+....*N..(....o.... (,...*&..(-....*.s.....s/.....s0.....s1.....s2.....*....0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0..<.....~..... (8.....,lr...p.....(9...o:....s;.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\outlook\outlook.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.692203118539672
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	UOB_BANK_MT104_SCAN.exe
File size:	818176
MD5:	62cffbe922a88ebae13ab4aebfd8ed2d
SHA1:	5693218467596783 08cb52d01537aefc2d9d8389
SHA256:	bcb425236d9708acd844d3abf15e14a33f029ee760d1dac f9c590a70c2283e75
SHA512:	c383b9420d22fd87aaedd9f5a157f8757abf53efb9d6ce72 4416ac26a4cbb21c59b7da7db2830b8f9f3b234b161dc02 6d25e55dc9f7d3d67df45c8fc7256f3c4
SSDEEP:	12288:SopTcgSA5FMxYj3yATy1nWPGNUsSvjHAE0diJ HXbms5PulZWYNh3Cq4HrRDi4DHL:PTNHgYjiA21WL7 PNas5PuyY/d4HNhmq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... E.t`.....P..\.....>z... .....@.. ....@.....

File Icon

Icon Hash:	1e3731393931371c

Static PE Info

General

Entrypoint:	0x4b7a3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60740445 [Mon Apr 12 08:26:45 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
or dword ptr [edx], ecx
or eax, 00000020h
add byte ptr [ecx+49h], cl
sub al, byte ptr [eax]

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
dec ebp
dec ebp
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb79ec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0x11a54	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb5a5c	0xb5c00	False	0.917843825224	data	7.89150282711	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x11a54	0x11c00	False	0.0690746038732	data	2.12909126826	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb8160	0x10828	data		
RT_GROUP_ICON	0xc8988	0x14	data		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0xc899c	0x14	data		
RT_VERSION	0xc89b0	0x37c	data		
RT_MANIFEST	0xc8d2c	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

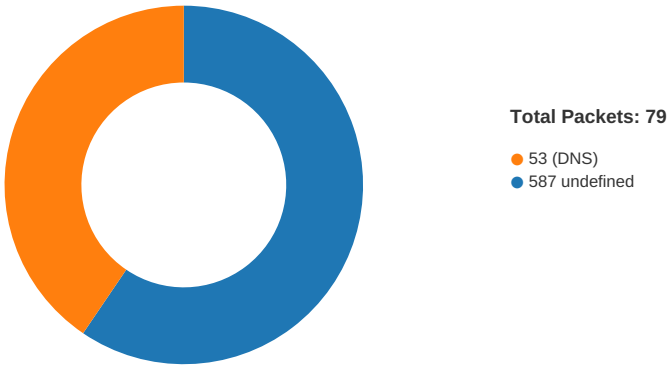
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Adobe Inc, Sel 2011 - 2021
Assembly Version	1.0.0.0
InternalName	UTF8Decoder.exe
FileVersion	1.0.0.0
CompanyName	Adobe Inc, Sel
LegalTrademarks	
Comments	
ProductName	Image Studio
ProductVersion	1.0.0.0
FileDescription	Image Studio
OriginalFilename	UTF8Decoder.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:43:44.088363886 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.175313950 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.175730944 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.416920900 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.417490005 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.506367922 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.506439924 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.507352114 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.594712973 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.637120962 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.677920103 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.768826008 CEST	587	49751	77.88.21.158	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:43:44.768860102 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.768894911 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.768919945 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.768955946 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.768991947 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.825815916 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:44.912899971 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:44.965246916 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.259609938 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.346306086 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.348658085 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.437921047 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.439239025 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.542537928 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.544009924 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.635410070 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.636209011 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.729252100 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.729968071 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.817075014 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.822437048 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.822658062 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.823342085 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.823451042 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:45.909910917 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:45.910979033 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:46.478163004 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:46.527929068 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:47.842917919 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:47.929693937 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:47.929750919 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:47.930035114 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:48.114232063 CEST	49751	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:48.202858925 CEST	587	49751	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.031492949 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.118124962 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.118231058 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.353441954 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.353651047 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.441134930 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.441169977 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.441395044 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.532269001 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.532725096 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.620734930 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.620768070 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.620789051 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.620806932 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.620877981 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.620942116 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.624454975 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.710761070 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.713831902 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.801517963 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.802402020 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.889991045 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.891146898 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:49.995840073 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:49.996519089 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.086659908 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.087469101 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.182554007 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.183394909 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.270052910 CEST	587	49753	77.88.21.158	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:43:50.272769928 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.273118973 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.273451090 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.273760080 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.274239063 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.274544954 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.274770975 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.275033951 CEST	49753	587	192.168.2.4	77.88.21.158
Apr 12, 2021 13:43:50.361502886 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.362443924 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.362487078 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.363063097 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.405034065 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.900011063 CEST	587	49753	77.88.21.158	192.168.2.4
Apr 12, 2021 13:43:50.950139999 CEST	49753	587	192.168.2.4	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:41:47.088049889 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:47.161422014 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:49.629338026 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:49.691839933 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:51.551294088 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:51.599951982 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:52.932041883 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:52.981076002 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:53.770360947 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:53.820811033 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:54.807579994 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:54.857723951 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:55.635274887 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:55.686678886 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 13:41:58.977431059 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:41:59.030529976 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:04.878201962 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:04.932564020 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:06.394237995 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:06.444811106 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:07.652136087 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:07.701169968 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:09.703676939 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:09.755377054 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:23.092509031 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:23.142779112 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:24.527841091 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:24.581901073 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:29.328098059 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:29.385510921 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:30.232234955 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:30.281128883 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:40.249526978 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:40.317590952 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:42.329910040 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:42.381172895 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:52.982672930 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:53.040520906 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 13:42:54.232973099 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:42:54.287647009 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:01.674324036 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:01.722995043 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:06.847794056 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:06.898809910 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:08.905364990 CEST	51255	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 13:43:08.967346907 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:23.779581070 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:23.831465006 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:26.071857929 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:26.131859064 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:26.888319969 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:26.940362930 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:42.477943897 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:42.526719093 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:43.810199022 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:43.872534990 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:43.896019936 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:43.956119061 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:44.370868921 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:44.439306974 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:48.537571907 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:48.599728107 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 13:43:48.970973969 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 13:43:49.030179024 CEST	53	59172	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 13:43:43.810199022 CEST	192.168.2.4	8.8.8.8	0xa1eb	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Apr 12, 2021 13:43:43.896019936 CEST	192.168.2.4	8.8.8.8	0xbc0	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Apr 12, 2021 13:43:48.537571907 CEST	192.168.2.4	8.8.8.8	0xa8c6	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Apr 12, 2021 13:43:48.970973969 CEST	192.168.2.4	8.8.8.8	0xe20c	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 13:43:43.872534990 CEST	8.8.8.8	192.168.2.4	0xa1eb	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 13:43:43.872534990 CEST	8.8.8.8	192.168.2.4	0xa1eb	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Apr 12, 2021 13:43:43.956119061 CEST	8.8.8.8	192.168.2.4	0xbc0	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 13:43:43.956119061 CEST	8.8.8.8	192.168.2.4	0xbc0	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Apr 12, 2021 13:43:48.599728107 CEST	8.8.8.8	192.168.2.4	0xa8c6	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 13:43:48.599728107 CEST	8.8.8.8	192.168.2.4	0xa8c6	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Apr 12, 2021 13:43:49.030179024 CEST	8.8.8.8	192.168.2.4	0xe20c	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 13:43:49.030179024 CEST	8.8.8.8	192.168.2.4	0xe20c	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

SMTP Packets

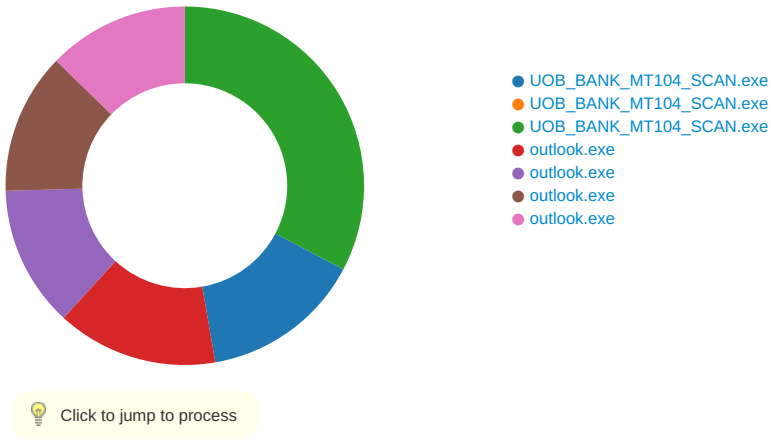
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 13:43:44.416920900 CEST	587	49751	77.88.21.158	192.168.2.4	220 myt4-1dda227af9a8.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Apr 12, 2021 13:43:44.417490005 CEST	49751	587	192.168.2.4	77.88.21.158	EHLO 571345

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 13:43:44.506439924 CEST	587	49751	77.88.21.158	192.168.2.4	250-myt4-1dda227af9a8.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Apr 12, 2021 13:43:44.507352114 CEST	49751	587	192.168.2.4	77.88.21.158	STARTTLS
Apr 12, 2021 13:43:44.594712973 CEST	587	49751	77.88.21.158	192.168.2.4	220 Go ahead
Apr 12, 2021 13:43:49.353441954 CEST	587	49753	77.88.21.158	192.168.2.4	220 iva8-174eb672ffa9.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Apr 12, 2021 13:43:49.353651047 CEST	49753	587	192.168.2.4	77.88.21.158	EHLO 571345
Apr 12, 2021 13:43:49.441169977 CEST	587	49753	77.88.21.158	192.168.2.4	250-iva8-174eb672ffa9.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Apr 12, 2021 13:43:49.441395044 CEST	49753	587	192.168.2.4	77.88.21.158	STARTTLS
Apr 12, 2021 13:43:49.532269001 CEST	587	49753	77.88.21.158	192.168.2.4	220 Go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: UOB_BANK_MT104_SCAN.exe PID: 7164 Parent PID: 6096

General

Start time:	13:41:53
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe'
Imagebase:	0x790000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.653990292.0000000003E9B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.653198971.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UOB_BANK_MT104_SCAN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UOB_BANK_MT104_SCAN.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: UOB_BANK_MT104_SCAN.exe PID: 976 Parent PID: 7164

General

Start time:	13:42:00
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
Imagebase:	0x150000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: UOB_BANK_MT104_SCAN.exe PID: 6460 Parent PID: 7164

General

Start time:	13:42:01
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\UOB_BANK_MT104_SCAN.exe
Imagebase:	0x9f0000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.901584866.00000000030E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.900779830.0000000002DE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.897472455.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming\outlook	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\outlook\outlook.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\outlook\outlook.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\voqu0pjl.ash	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C22DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome\Default\Cookies	success or wait	1	6C226A95	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\outlook\outlook.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 45 04 74 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 5c 0b 00 00 1e 01 00 00 00 00 00 3e 7a 0b 00 00 20 00 00 00 80 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...E.t`.......... ....P..\..........>z... ....@.. ....@................	success or wait	4	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\outlook\outlook.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C22DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\b6e02eea-b530-48f6-b606-1d15259be23a	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\voqu0pjl.ash\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C221B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	outlook	unicode	C:\Users\user\AppData\Roaming\outlook\outlook.exe	success or wait	1	6C22646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	outlook	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C22DE2E	RegSetValueExW

Analysis Process: outlook.exe PID: 5832 Parent PID: 3424

General

Start time:	13:42:33
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\outlook\outlook.exe'
Imagebase:	0x4f0000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.734707746.0000000002901000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.736717665.0000000003A8B000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\outlook.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: outlook.exe PID: 5948 Parent PID: 5832

General

Start time:	13:42:39
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Imagebase:	0x6c0000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.897512703.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.900334677.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.900334677.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: outlook.exe PID: 4684 Parent PID: 3424

General

Start time:	13:42:42
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\outlook\outlook.exe'
Imagebase:	0xa00000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.759764296.000000000408B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.758186038.0000000002F01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: outlook.exe PID: 6832 Parent PID: 4684

General

Start time:	13:42:49
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\outlook\outlook.exe
Imagebase:	0xfb0000
File size:	818176 bytes
MD5 hash:	62CFFBE922A88EBAE13AB4AEBFD8ED2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.897512069.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.900125082.0000000003501000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Disassembly

Code Analysis